

REMARKS

In the Office Action, the Examiner rejected Claims 1-42, which were all of the then pending claims, under 35 U.S.C. 103 as being unpatentable over the prior art, and further rejected Claims 34-36 under 35 U.S.C. 112 as being indefinite. With respect to the rejections of the claims under 35 U.S.C. 103, Claims 1-5, 7-23 and 26-42 were rejected as being unpatentable over U.S. Patent 6,453,296 (Iwamura) in view of a document "Introducing Trusted Third Parties to the Mobile Agent Paradigm" (Wilhelm, et al.). Claims 6, 24, and 25 were rejected as being unpatentable over Iwamura in view of Wilhelm, et al. and further in view of U.S. Patent 6,714,982 (McDonough, et al.).

Applicants herein ask that independent Claims 1, 31, 33, 34, 37 and 40 be amended to better define the subject matters of these claims. Also, Claims 23 and 24 are being cancelled, and new Claims 43 and 44 are being substituted therefor to describe preferred features of the invention.

For the reasons discussed below, Claims 34-36 fully comply with 35 U.S.C. 112, and all of Claims 1-22 and 25-44 patentably distinguish over the prior art and are allowable. The Examiner is, hence, asked to enter this Amendment, to reconsider and to withdraw the rejection of Claims 34-36 under 35 U.S.C. 112 and the rejections of Claims 1-22 and 25-42 under 35 U.S.C. 103, and to allow Claims 1-22 and 25-44.

In rejecting Claims 34-36 under 35 U.S.C. 112, the Examiner noted that Claim 34 includes a reference to "the server" without being clear as to whether this server refers to the web server or the co-server. To address this, Applicants ask that Claim 34 be amended to change "the server" to "the co-server". It is believed that this corrects the informality noted by the Examiner, and the

Examiner is thus requested to reconsider and to withdraw the rejection of Claims 34-36 under 35 U.S.C. 112.

With regard to the rejections of the claims over the prior art, Applicants respectfully submit that the pending claims are patentable because the prior art does not disclose or suggest using a trusted co-server, as described in the independent Claims 1, 31, 33, 34, 37 and 40, to verify the authenticity of interactions between the client and a server.

To elaborate, the present invention enables a server operator, operating within the existing SSL and Web infrastructure, to provide services with security properties that a remote user can verify, even if the server operator may have a reason or motivation to subvert those properties.

Iwamura describes a special purpose distributed system to support a particular agency's commerce application, and this system uses shared secrets and has the agency distribute secret keys, which make it impossible for the parties involved to prove non-repudiation. There is no means disclosed in Iwamura, however, for any party to verify that the information at the other end is protected and properly assembled or to prove these properties to a third party.

An important feature of the preferred embodiment of this invention is that the secure application software, loaded into a secure co-processor, can turn around and prove itself - that is, that it is the software running inside untampered hardware - to arbitrary third parties using public-key cryptography. This feature is discussed on pages 16 and 17 of the present application. In addition, the present invention, in its preferred implementation, is able to prove itself within the current SSL infrastructure, through a standard Certificate Authority.

Wilhelm discloses tamper-resistant hardware with a manufacture-certified key pair. However, Wilhelm uses this key pair to enable a remote shipper of an agent to ship the agent

encrypted to the hardware. Once decrypted, the agent can use secrets it carried with it to authenticate back to the shipper. The preferred embodiment of the present invention, in contrast, uses the key pair itself to authenticate the code that resides in the hardware. This approach lets the code arrive unencrypted, and allows the relying party to be anyone. Moreover, the system of the present invention does not require mobile agents that move between agent hosts. Rather, the present invention, preferably, uses static Web server applications that interact with multiple remote parties using standard browsers, not special agent nodes.

Independent Claims 1, 31, 33, 34, 37 and 40 each describe the feature of using a trusted co-server as a trusted third party to authenticate interactions between the client and the server. This feature is of significant utility because it enables a universal infrastructure that supports myriad applications from multiple server operators. The invention permits the additional flexibility of allowing the server operator, remote users, server application developers, hardware manufacturers, and SSL CAs all to be separate parties.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, also fail to disclose or teach the use of the trusted co-server in the manner described in Claims 1, 31, 33, 34, 37 and 40.

For instance, McDonough does not teach how the users can verify that the server operator is not lying or mistaken when the server operator claims the scanning has been performed.

Because of the above-discussed differences between Claims 1, 31, 33, 34, 37 and 40 and the prior art, and because of the advantages associated with those differences, these claims patentably distinguish over the prior art and are allowable. Claims 2-22, 25-30, 43 and 44 are dependent from Claim 1 and are allowable therewith. Claim 32 is dependent from, and is

allowable with, Claim 31; and Claims 35 and 36 are dependent from Claim 34 and are allowable therewith. Claims 38 and 39 are dependent from, and are allowable with Claim 37, and Claims 41 and 42 are dependent from Claim 40 and are allowable therewith.

It is noted that the changes requested herein to Claims 1, 31, 33, 34, 37 and 40 elaborate on features already described in these claims. Specifically, each of these claims already describes a trusted co-server, and the claims are being amended to describe in more detail the function of that co-server. Accordingly, it is believed that entry of this Amendment is appropriate, and such entry is respectfully requested.

For the reasons discussed above, the Examiner is asked to enter this Amendment, to reconsider and to withdraw the rejections of Claims 34-36 under 35 U.S.C. 112, and the rejections of Claims 1-22 and 25-42 under 35 U.S.C. 103, and to allow Claims 1-22 and 25-44. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,

John S. Sensny
John S. Sensny
Registration No. 28,757
Attorney for Applicants

Scully, Scott, Murphy & Presser
400 Garden City Plaza – Suite 300
Garden City, New York 11530
(516) 742-4343

JSS:jy